INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Spain

López-Ibor DPM Abogados is a prestigious and international full-service Spanish law firm with strategic offices in Madrid, Barcelona and Valencia.

López-Ibor DPM Abogados has been recognized as a leading full-service firm by the most prestigious international rankings such as Chambers & Partners, Legal 500, IFLR1000, World Tax and Best Lawyers.

Our commitment to excellence is built on a foundation of extensive experience and a track record of success. With a legacy that extends over many years, our firm has consistently delivered unique solutions to a diverse range of legal challenges. What sets us apart is the unwavering loyalty and closeness demonstrated by our clients, reflecting the trust they place in our expertise.

At López-Ibor DPM Abogados, we offer comprehensive legal counsel across various domains, including Corporate and Commercial Law, Intellectual Property, Employment Law, Taxation and New Technologies.

Our specialized New Technologies department focuses on safeguarding personal data, e-commerce, and social media. This encompasses professional support in crafting privacy policies, general terms of sale for online stores, and terms of use for websites. We also provide legal assistance in online contracting, commercial activities, advertising, Internet and social media, protection of intellectual property rights, and issues related to labor law in the realm of new technologies. Notably, we have successfully addressed cybercrimes committed by hackers through online interventions.

Furthermore, our expertise extends to data protection regulations, where we offer timely advice to ensure compliance with the General Data Protection Regulation (GDPR). We meticulously review companies' internal policies and procedures concerning data protection, aligning

Contact Us

+34 915 21 78 18
https://lopez-iborabogados.com/en/
jaime.morey@l-ia.com
López de Hoyos 35, 3º
Madrid, 28002 Spain

them with the latest Spanish and European regulations. Our thorough examination of contracts ensures the incorporation of clauses pertaining to data protection and confidentiality, tailored to the nature of each agreement.

At López-Ibor DPM Abogados, we pride ourselves on being at the forefront of legal innovation, providing steadfast support to our clients in navigating the complexities of contemporary legal landscapes.

Introduction

We have compiled the main differences between the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR") and the local Spanish Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights, mentioning only the differences where the Spanish legislation has added or modified some of the rights and provisions of the aforementioned European regulation.

In the following headings and subheadings, we will only address the points where there are noteworthy differences in the Spanish legislation with respect to the GDPR. We will not include any content to the headings and subheadings where there are no particularities in the Spanish legislation with respect to the GDPR.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The **Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and guarantee of digital rights** (hereinafter, "**Spanish DP Law**") is the Spanish national law that transposed and incorporated the provisions of the GDPR and is effective in the whole territory of Spain.

2.2. Additional or ancillary regulation, directives or norms

The recent **Law 11/2023**, of May 8, (the "Law 11/2023"), which transposes several European Union Directives and amends several regulations, introduces some changes in the Spanish DP Law. The amendments, effective as from the day after the publication of the Law 11/2023, are aimed at modernizing and streamlining the procedures and deadlines before the Spanish Data Protection Agency in defense of the rights of citizens.

2.3. Upcoming or proposed legislation (if applicable)

There is no upcoming proposed legislation to amend the Spanish DP Law but considering the fast pace of new technology and AI, we should expect new modifications to the original text in the following years.

Scope of Application

3.1. Legislative Scope

Spanish DP Law is applicable in the geographical boundaries of Spain, exclusively impacting activities within the country. In contrast, the GDPR operates on a broader scale, encompassing all of the Member States of the European Union. Within the GDPR framework, each Member State has the capacity of implementing its particular legislation.

This autonomy enables Member States to adjust, tailor, or expand certain rights and obligations outlined in the GDPR to suit their specific legal and cultural contexts. In essence, while the Spanish DP Law pertains solely to Spain, the GDPR establishes a comprehensive foundation for data protection across the European Union, fostering a harmonized yet adaptable regulatory framework.

3.1.1.Definition of personal data

3.1.2. Definition of different categories of personal data

3.1.3. Treatment of data and its different categories

- *Regulation of personal and non-personal data*
- *Regulation of electronic and non-electronic data*
-

3.1.4. Other key definitions pertaining to data and its processing

3.2. Statutory exemptions

3.3. Territorial and extra-territorial application

Article 3(2) of the GDPR, establishes a series of cases in which controllers or processors of personal data located outside the European Union (EU) may be subject to the rules established in the GDPR, to the monitoring of the processing by the authorities of EU Member States such as Spain, and to its sanctioning regime.

Entities that, regardless of their location and nationality, carried out business activities in the EU with access to, and processing of, personal data of EU citizens, may be required to comply with European data protection rules, such as the Spanish DP Law.

For instance, any data subject residing in Spain, such as an American or Chinese citizen, if their data is being processed by a company not established in the EU, they will still be protected under the Spanish DP Law, specifically when:

- the processing of the data is in connection with the offering of goods or services to data subjects in the EU, regardless of whether the data subjects are required to pay for them; or

- the data processing is related to the monitoring of the behavior of data subjects, to the extent that the processing takes place in the EU.

Accordingly, Article 70.1(c) of the Spanish DP Law establishes that representatives of controllers or processors not established in the territory of the European Union are subject to the sanctioning regime established in the GDPR and the Spanish DP Law.

https://lopez-iborabogados.com/en/

Legislative Framework

4.1. Key stakeholders

Data Protection Officer (DPO)

In Article 37, the GDPR broadly outlines the criteria and circumstances for the appointment of a Data Protection Officer ("DPO") within an organization. Conversely, the Spanish DP Law delves deeper by enumerating a specific list of organizations which are obliged to designate a DPO, surpassing the general guidelines provided by the GDPR. This expanded list includes entities such as professional associations and their overarching councils, educational institutions,

providers of information society services, as well as insurance and financial services entities, among others.

The Spanish DP Law, therefore, extends the scope of DPO requirements beyond the parameters established in the GDPR, outlining a more detailed and nuanced set of criteria applicable to specific sectors and contexts.

Records of processing activities

GDPR, in its article 30, stipulates that "Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility", however, it would not apply to "an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data".

The legal framework in Spain, as articulated in the Spanish DP Law, introduces an additional requirement for certain organizations or entities. According to this provision, such entities are obliged to publicly disclose and publish a comprehensive inventory of their data processing activities. This disclosure must be easily accessible through electronic means, encompassing all the details specified in Article 30 of the GDPR. In essence, the Spanish DP Law extends beyond the GDPR by specifically stipulating the obligation for certain entities to proactively share and maintain a transparent record of their data processing endeavors, thereby fostering greater accountability and accessibility. Usually, these organizations will be public or administrative.

Among the organizations listed we can mention:

- Courts of Justice
- The National Bank of Spain ("Banco de España")
- Public universities
- Parliamentary groups
- Public bodies and public law entities.
- State Administration

4.2. Role and responsibilities of key stakeholders

Requirements for Data Processing

5.1. Grounds for collection and processing

- *Consent*
- *Consent Notice*
- *Withdrawal of Consent*

5.2. Data storage and retention timelines

5.3. Data correction, completion, updating or erasure of data

5.4. Data protection and security practices and procedures

5.5. Disclosure, sharing and transfer of data

5.6. Cross border transfer of data

5.7. Grievance redressal

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

- *Right to withdraw consent*
- *Right to grievance redressal and appeal*
- *Right to access information*
- *Right to nominate*

6.2. Duties

Processing of Children or Minors' data

The GDPR sets an age limit for the lawful processing of children's personal data; thus, data processing is considered lawful in Europe when the child is at least 16 years old.

The GDPR grants each Member State the freedom to independently determine a lower age for obtaining a child's consent in information society services. Nevertheless, it imposes a minimum limit of 13 years old; hence, no Member State is permitted to set the minimum age for consent below 13 years old.

In the case of Spain, article 7 of the Spanish DP Law has established the age at 14 years old, lowering the 16-year-old age determined under the GDPR.

Despite the Spanish age limit of 14 years there is an exception when the act or legal transaction that the child wants to carry out requires the authorization of the parents or guardians, whose consent for processing must be sought. Any type of online retail shopping would be an example of such act or legal transaction where this exception would apply.

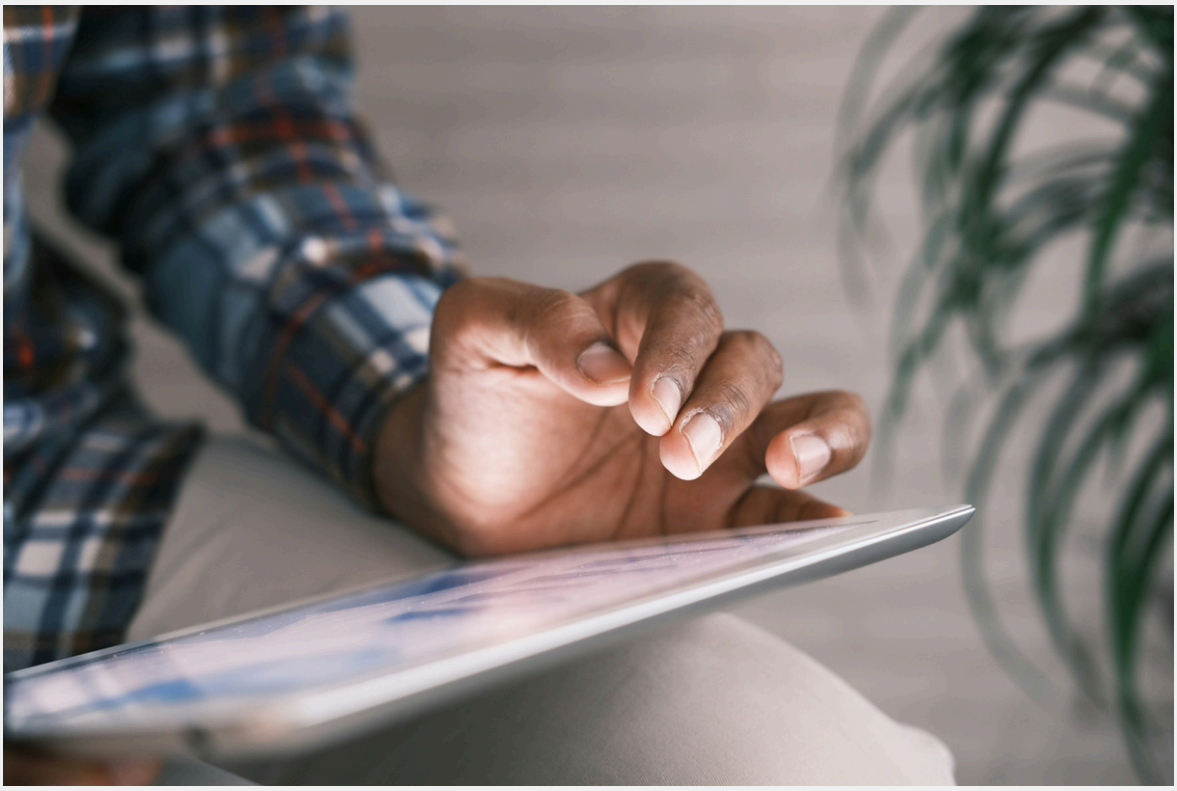
Regulatory Authorities

8.1. Overview of relevant statutory authorities

Each Member State is obliged to create their own internal authority to oversee the data protection in the country.

Under article 44 of the Spanish DP Law the Spanish Data Protection Agency ("Agencia Española de Protección de Datos", "AEPD") is the statutory authority with jurisdiction in data protection matters in the country.

AEPD stands as an independent administrative authority with nationwide jurisdiction, as outlined in Law 40/2015, dated October 1, which governs the Legal Regime of the Public Sector. The AEPD has legal personality and enjoys both public and private capacities, operates autonomously and is independent from other public authorities in the execution of its duties. Its formal link with the government is established through the Ministry of Justice. Additionally, the AEPD assumes the role of representative of all the data protection authorities within the Kingdom of Spain in front of the European Data Protection Committee.



8.2. Role, functions and powers of authorities

- Role functions and powers of principal data regulation authority (if applicable)

One of the primary responsibilities of the AEPD is to oversee the application of both the Spanish DP Law and the GDPR. Specifically, it is tasked with executing the functions described under Article 57 and wielding the powers listed under Article 58 of the GDPR, as well as those stipulated in the Spanish DP Law and its associated implementing provisions.

Furthermore, the AEPD assumes the duty of carrying out functions and exercising powers delegated to it by other laws or regulations within the framework of European Union Law. This multifaceted role underscores the AEPD's pivotal position in upholding data protection standards, both nationally and within the broader European context.

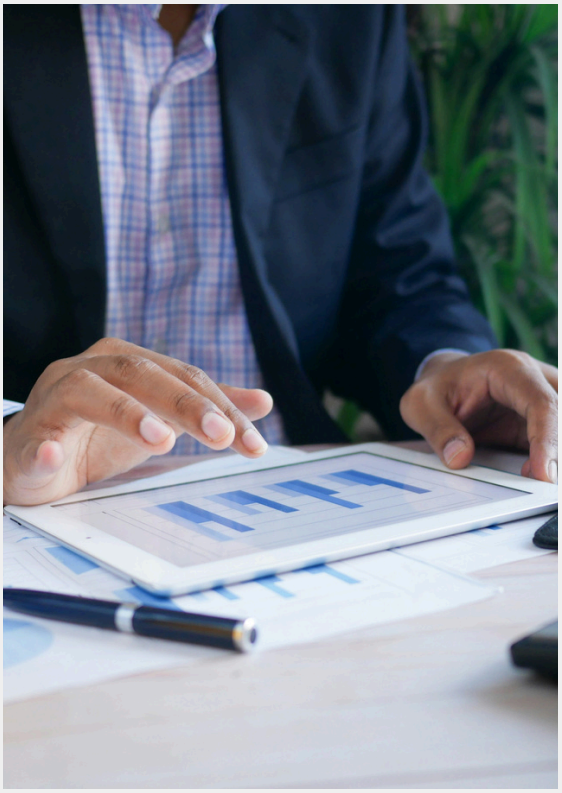
- Role, functions and powers of additional or ancillary data regulation authorities (if applicable).

As of today, there are three regional data regulation authorities: the Catalan Data Protection Authority, the Basque Data Protection Agency and the Council for Transparency and Data Protection of Andalusia. The latter was created in 2014, with the special feature that in this region ("Comunidad Autónoma"), the competent entity in data protection

matters is also competent in transparency matters.

Each one of them has particular functions for their own regions, which mainly involves monitoring the application of the data protection regulation in their territory and specially when entities of the public sector of those regions are involved in the data processing.

Nevertheless, the AEPD continues to serve as the overseeing authority across the entire territory, encompassing the three aforementioned regions with which it collaborates and enforces mechanisms for coherence.



8.3. Role, functions and powers of civil/criminal courts in the field of data regulation

The Central Administrative Courts ("Juzgados Centrales de lo Contencioso-Administrativo") are responsible for authorizing, by means of an order, the requests for information issued by the AEPD and other independent administrative authorities at the state level to operators providing publicly available electronic communications services and providers of information society services, when this is necessary in accordance with the Spanish DP Law.

Moreover, the Contentious-Administrative Section of the Supreme Court will decide about the request for authorization for the declaration provided for in the Fifth Additional Provision of the Spanish DP Law, when such request is made by the General Council of the Judiciary ("Consejo General del Poder Judicial").

Such Fifth Additional Provision of the Spanish DP Law refers to the judicial authorization in relation to decisions of the European Commission on international transfer of data.

Finally, the Contentious-Administrative Section of the National Audience ("Audiencia Nacional") will also decide about the request for authorization for the declaration provided for in the Fifth Additional Provision of the Spanish DP Law, when such request is made by the AEPD.

Consequences of non-compliance

9.1. Consequences and penalties for data breach

Sanctions and penalties under the General Data Protection Regulation (GDPR) and the Spanish DP Law share foundational principles but exhibit nuanced distinctions. Within the overarching framework, both regulations empower regulatory authorities to impose fines for breaches, yet their specific applications diverge to some extent.

In the broader spectrum, the GDPR provides a comprehensive foundation for penalties, delineating a general framework that allows for substantial fines as a response to infringements. The maximum penalty, levied for severe violations, can reach up to 4% of the global annual turnover or EUR 20,000,000.-, depending on which amount is greater. This regulation incorporates a flexible approach, recognizing the varied nature and seriousness of potential violations.

Conversely, the Spanish DP Law maintains a parallel structure while introducing specificities tailored to the Spanish legal context. Although aligned with the GDPR's fundamental principles, the Spanish DP Law contains different provisions concerning the imposition of

penalties within the Spanish territory. This includes the determination of specific fine amounts, reflecting the legislation's commitment to addressing data protection breaches, specifically for Spain.

While the GDPR lays out general criteria for imposing fines, considering factors such as the nature, severity and duration of the violation, the Spanish DP Law adapts these criteria to align them with the Spanish legal system. It provides a tool through which authorities can assess breaches, acknowledging the unique circumstances that may arise within Spain's regulatory framework. For instance, Spanish DP Law specifically includes a statute of time limitation period depending on the amount of the fines, ranging from one (1) to three (3) years.

Therefore, while the fundamental concept of imposing penalties for data protection breaches remains consistent throughout the GDPR, the Spanish DP Law contains particularities to ensure an effective, contextually relevant application of sanctions within its jurisdiction.

9.2. Consequences and penalties for other violations and non-compliance

Conclusion

In conclusion, the examination of the Spanish DP Law in contrast to the General Data Protection Regulation (GDPR) has raised certain particularities which underscore the particular approach and nuanced framework established by Spanish legislation. The following are, in summary, the most important differences:

A. Different Age of Consent:
Spanish DP Law has introduced a distinctive age threshold for the valid consent of minors, setting it at the age of 14 years. This deviation from the GDPR's uniform age requirement reflects Spain's emphasis on tailoring regulations to specific cultural and social contexts.

B. Designation of a Data Protection Officer (DPO) for Public Authorities:
Spanish regulations uniquely oblige the appointment of a DPO for public authorities and entities, irrespective of their size. This proactive measure reflects a commitment to enhancing accountability and compliance within the public sector.

C. Sanctioning Authority:
In Spain, the AEPD assumes a central role as the principal authority responsible for imposing sanctions for data protection infringements. This specific delineation differs from the decentralized approach under the GDPR, where different supervisory authorities in each EU Member State are empowered to impose sanctions independently.

These identified nuances underscore the importance of understanding the intricacies of the Spanish data protection legal framework. As businesses and entities navigate the complexities of compliance, awareness of these distinctive

features is important to ensure comprehensive adherence to both the Spanish DP law and the broader GDPR.

If you wish to expand on the content of this article or need advice in relation to the Spanish Data Protection regulations, we would be very pleased to assist, and you can contact us any time:

Jaime Morey:
jaime.morey@l-ia.com

Pablo Stöger:
pablo.stoger@l-ia.com

Alfonso López-Ibor:
alfonso.lopezibor@l-ia.com

Kevin Alfonso:
kevin.alfonso@l-ia.com

Contact Us

+34 91 52 17 818

www.lopez-iborabogados.com

jaime.morey@l-ia.com

Calle López de Hoyos, 35, 3º
E-28002 Madrid (Spain)